Office of Inspector General

Audit Report

Controls Over Airport Identification Media

Federal Aviation Administration

Report No.: AV-2001-010
Date Issued: December 7, 2000

Memorandum

U.S. Department of Transportation

Office of the Secretary of Transportation

Office of Inspector General

Subject: ACTION: Report on Audit of Controls Over Airport Identification Media Federal Aviation Administration AV-2001-010

Date: December 7, 2000

From: Alexis M. Stefani
Assistant Inspector General for Auditing

Reply to Attn of: JA-10

To: Federal Aviation Administrator

This report presents the results of the audit of Controls Over Airport Identification Media. The objective of the audit was to determine whether Federal Aviation Administration (FAA) requirements for airport identification media (airport ID) ensure that only individuals who can be trusted with the public safety are granted access to secure airport areas. An executive summary of the report follows this memorandum. A draft of this report was provided to FAA on August 4, 2000, and FAA's August 25, 2000 comments were considered in preparing this final report.

The draft report contained nine recommendations designed to improve controls over airport ID. Two of the recommendations were included in the Airport Security Improvement Act of 2000 (Public Law 106-528), which was signed by the President on November 22, 2000. FAA concurred with all recommendations except one. FAA partially concurred with the recommendation to use foreign criminal checks, credit checks and drug tests to help assess whether individuals can be trusted with the public's safety and be permitted to work in secure airport areas. FAA commented that there are significant problems with conducting and using foreign criminal checks. Based on FAA's comments, we revised our final report and removed the portion of the recommendation related to using foreign criminal checks in employee background investigations.

With respect to requiring credit checks and drug tests, FAA stated that it would work with Congress, industry, and the law enforcement community to determine if they can be fully or partially implemented. However, to ensure that concrete progress is made in addressing this recommendation, FAA needs to provide a target

date for the review and implementation of any requirements for using credit checks and drug tests in employee background investigations.

FAA planned corrective actions were adequate to resolve the other eight recommendations. However, as more fully discussed in the body of the report, estimated completion dates are needed for four of the eight recommendations. We request that you provide estimated completion dates for the recommendations within 15 days. The remaining four recommendations are considered resolved subject to the follow-up provisions of Department of Transportation Order 8000.1C.

This report is marked sensitive security information in its entirety and is therefore subject to the disclosure restrictions outlined in Title 14 Code of Federal Regulations Part 191.

We appreciate the cooperation and assistance provided by your staff during the audit. If I can answer any questions or be of further assistance, please contact me at (202) 366-1992, or David A. Dobbs, Deputy Assistant Inspector General for Aviation, at (202) 366-0500.

#

cc: Carl Burleson, AOA-2
Donna McLean, ABA-1
Ronald Page, ABU-100

EXECUTIVE SUMMARY

Controls Over Airport Identification Media

Federal Aviation Administration

OBJECTIVE

The objective of the audit was to determine whether Federal Aviation Administration (FAA) requirements ensure that only individuals who can be trusted with the public's safety are granted access to secure[1] airport areas. We also assessed FAA's oversight of airport operator and air carrier procedures for issuing and accounting for airport identification media (airport ID[2]) used to access secure airport areas. Further, we reviewed airport operators' and air carriers' compliance with airport ID requirements.

BACKGROUND

U.S. airport operators are required to implement FAA-approved security programs. The security programs must include a system, method or procedure for controlling access to the secured area[3] that: (1) ensures only authorized individuals gain access to secured areas; (2) immediately denies access to individuals whose authority changes, such as former employees; (3) differentiates between individuals with unlimited access to the secured area and individuals with only partial access; and (4) has the capability of limiting an individual's access by time and date. Over 450 airports are subject to the requirement and have FAA-approved security programs.

To ensure that only authorized individuals gain access to secure areas, airport operators and air carriers are required to conduct employment history investigations (background investigations) before issuing airport ID. To ensure that access to secure airport areas is denied immediately to individuals whose authority changes, airport security programs must include a process requiring

[1] OIG defines **"secure area"** as the area of an airport where each person is subject to a background investigation and required to display airport-approved identification. Each airport defines this area, which may be the entire Air Operations Area (AOA) or may be limited to a smaller, more restrictive area.

[2] OIG defines **"airport ID"** as all media issued to individuals to permit access to secure areas.

[3] The **secured area** (versus secure area) is the portion of an airport where passengers board and deboard aircraft, and the area surrounding the aircraft. In terms of access control, it must be the most secure area within the AOA.

immediate notification to the airport operator when employees[4] no longer require access.

RESULTS-IN-BRIEF

Controlling access to secure airport areas has been, and continues to be, an area of great concern due to increased threat to U.S. airport facilities. Two important access control requirements are to limit access to secure airport areas to only individuals who can be trusted with the public's safety and immediately deny access when an individual's authority changes. FAA has not taken adequate steps to ensure these requirements are met. Specifically:

- FAA's background investigation requirements for issuing airport ID are ineffective because they do not accomplish their intended purpose of providing adequate assurance that individuals who are granted unescorted access to secure airport areas can be trusted with the public's safety. For example, Federal Bureau of Investigations (FBI) criminal record checks (criminal checks) are only required for individuals applying for airport ID when one of four conditions triggers the checks. One of the triggers, a 12-month unexplained gap in employment, was designed to identify individuals who were incarcerated for committing a serious crime. However, we found that the trigger is ineffective because not all individuals convicted of serious crimes have a 12-month gap in employment.

  In March and April 2000, we testified before the House and Senate on our results. At that time, bills were introduced to strengthen background investigation requirements. In November, the President signed the Airport Security Improvement Act of 2000 (Public Law 106-528), which will strengthen background investigation requirements. FAA and the airport industry have stated support for the legislation. To further help determine the trustworthiness of employees, FAA should consider using other investigative tools, such as credit checks and drug tests, to determine whether individuals are trustworthy, as well as conducting randomly recurring criminal checks for existing employees.

- Until new requirements are established, industry must comply with existing requirements. However,

Airport users include foreign air carriers, non-air-carrier airport tenants, and companies that do not have offices at the airport, but require access to the airport's secure area.

[4] In this report, we use the term employees to mean all individuals authorized unescorted access to secure airport areas, whether these individuals are employed by airports, air carriers, or other entities conducting business at airports.

we determined that background investigation requirements were frequently not followed by airport operators, air carriers and airport users. For 35 percent of the employees randomly selected for review at six airports, we found no evidence (19 percent) or incomplete evidence (16 percent) that background investigations were performed as required. In addition, recent investigations resulted in fining two companies doing business at major U.S. airports for falsely certifying that background investigations were performed when, in fact, they were not. One of the companies was ordered by a U.S. District Judge to pay more than $1.5 million for allowing untrained employees, some with criminal backgrounds including drug dealing, kidnapping, aggravated assault and theft, to operate security checkpoints.

- Until the background investigation regulations are changed, FAA needs to ensure industry's compliance with requirements. We found that FAA's oversight of air carriers' and airport users' compliance with current regulations needs improvement. For example, FAA's previous national assessments of compliance mainly focused on airport users at 20 major U.S. airports, and for the airports we reviewed, the actions taken by FAA to correct the deficiencies identified during the assessments were not always effective.

- Also, FAA should issue the planned revision to regulations, which will require airport operators and air carriers to audit active airport IDs at least once a year. FAA must also issue standard audit procedures to ensure these audits are effective. We determined that airport operators had not developed and implemented adequate procedures to account for airport ID and immediately deny access to secure airport areas when required. At the 6 airports reviewed, we found that 9 percent (234 of 2,586 reviewed) of the IDs issued for access to secure airport areas remained active, even though the employee's authority had changed and access was no longer required.

EXECUTIVE SUMMARY

PRINCIPAL FINDINGS

Improvements Needed in FAA Requirements for Issuing Airport ID

FAA requires airport operators and air carriers to conduct background investigations before issuing airport ID authorizing access to secure airport areas. The background investigation procedures include: obtaining a 10-year employment history from those applying for access; verifying the most recent 5 years of that history; and performing an FBI criminal check when specific conditions are identified. Individuals convicted within the past 10 years of any of 25 enumerated crimes are denied airport ID. (See Exhibit A for the list of disqualifying crimes.)

Conditions that trigger an FBI criminal check are (1) an unexplained gap of employment for 12 months or more, (2) inability to substantiate statements made, (3) significant inconsistencies between information provided by the applicant and information obtained during the background investigation, and (4) information becomes available during the background investigation indicating a possible conviction for a disqualifying crime.

FAA's Regulations Are Ineffective

Background investigations based on FAA's regulations prove, in most cases, only the identity of the person applying for airport ID and, in limited instances when a criminal check is required, whether the FBI has a record of conviction for a disqualifying crime within the past 10 years. They do not provide adequate assurance that the individual can be trusted with the public's safety, which is the intended purpose of conducting background investigations. We found the following deficiencies in FAA's background investigation regulations.

- ***FBI criminal checks are only required for individuals applying for airport ID when one of four conditions triggers the checks.*** One of the triggers, a 12-month unexplained gap in employment, was designed to identify individuals who were incarcerated for committing a serious crime. However, we found that the trigger is ineffective because not all individuals convicted of serious crimes have a 12-month gap in employment. For example, according to U.S. Department of Justice statistics published in July 1999, 61 percent of all state and Federal felony convictions resulted in probation or an average jail sentence of 6 months. Even for violent felonies, 43 percent of convictions resulted in probation or an average jail sentence of just 7 months.

EXECUTIVE SUMMARY

- ***The list of 25 crimes that disqualified an individual from being issued airport ID was insufficient and did not include serious crimes, such as assault with a deadly weapon, unarmed robbery, burglary, larceny, and possession of drugs.*** Our analysis of 53 employees issued airport ID and arrested in a recent Department of Justice airport investigation for smuggling contraband on commercial aircraft, showed that individuals convicted of disqualifying crimes were not the only employees who presented a security risk. Of the 15 (28 percent) arrested employees with FBI criminal records, just one had a criminal record for a disqualifying crime (committed after being issued airport ID). Other arrested employees (14) had FBI criminal records for non-disqualifying felonies, such as larceny, battery, possession of a stolen vehicle, possession of drugs, and credit card fraud.

- ***FBI criminal checks were not recurring.*** FAA does not require recurring criminal checks but relies on air carriers, airport users, and employees to report employees convicted of disqualifying crimes to airport operators so that access to secure areas can be immediately denied to those individuals. Our analysis of the 53 employees arrested in the recent Department of Justice investigation found that 9 employees were charged with crimes after being issued airport ID, including 1 individual charged with a disqualifying crime. Criminal checks must be recurring to ensure the continued trustworthiness of employees.

FAA has the authority to require criminal checks for all employees and to expand the list of disqualifying crimes. In February 1992, FAA proposed requiring a criminal check for all employees. However, industry opposed the proposal based on a number of factors, including its cost and the impracticality of escorting personnel while waiting for results of a criminal check. In 1992, performing a criminal check took up to 90 days. Today, technology allows the criminal check to be completed in only a few days.

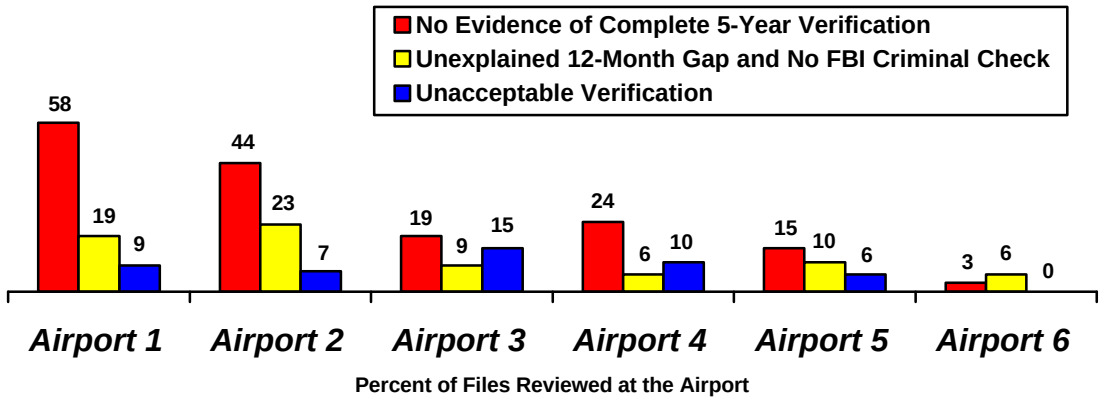
In October of this year, Congress passed the Airport Security Improvement Act of 2000 (Public Law 106-528), which was signed by the President on November 22, 2000. The legislation requires criminal checks for all employees and expands the list of disqualifying crimes. As a result of the technology advancements and quicker processing time, FAA and industry representatives support these initiatives. In fact, FAA is currently testing the new technology in a pilot program. We support these initiatives and recommend that FAA issue new rules requiring initial and randomly recurring criminal checks for all employees.

FAA should also consider requiring credit checks and drug tests as investigative tools. Some U.S. and foreign jobs require these types of checks and tests to help determine the trustworthiness of employees.

Airport Operators, Air Carriers and Airport Users Did Not Comply With Background Investigation Requirements

Although background investigation requirements need to be revised, it is important that airport operators, air carriers and airport users comply with current requirements. Our recent work at six airports found that these requirements were not being met. For 35 percent of the employee files reviewed, there was no evidence (19 percent) or incomplete evidence (16 percent) that a background investigation was performed as required. Despite the employers' failure to comply with security requirements, the individuals were issued airport ID and granted access to secure airport areas.

Also, 15 percent of the employee files reviewed showed an unexplained gap of employment of 12 months or more, but the required FBI criminal check was not performed. Further, 9 percent of the background verifications we reviewed used an unacceptable method, such as verifying an employee's background with a personal reference or family member. The chart below summarizes the specific noncompliance with background investigation requirements for the six airports reviewed.



The most serious noncompliance was at Airports 1 and 2, which permitted airport users to self-certify that background investigations were performed but had not established controls to ensure the investigations were properly completed. For example, 58 percent of the employee files reviewed at Airport 1 did not have evidence that a complete verification was conducted of the employee's most recent 5-year employment history. In contrast, Airport 6, with the lowest rate of noncompliance, did not permit airport users to self-certify that background investigations were performed.

EXECUTIVE SUMMARY

FAA Had Not Taken Effective and Timely Actions to Ensure Compliance

We found FAA's national assessments of compliance with background investigation requirements mainly focused on airport users at 20 major U.S. airports and actions to correct airport systemic problems were not always taken. For example, at least two of three FAA national assessments included two of the five airports we reviewed that permitted airport users to self-certify that background investigations were performed. We found significant problems continued at both airports due to inadequate controls. Air carrier compliance was not formally reviewed until fiscal year (FY) 1999. After we completed our audit fieldwork, FAA initiated a broad-scoped national review of compliance.

Also, FAA's airport assessments of compliance with background investigation requirements need improvement. For example, we analyzed annual airport assessments, with respect to assessing compliance with background investigation requirements, for the six airports reviewed for FYs 1997, 1998 and 1999. We found the assessments of compliance with background investigation requirements were not always made or were limited in scope.

Further, FAA was slow to implement new requirements and consistently failed to issue timely and adequate guidance to implement existing requirements. For example, FAA had not completed steps until May 2000 to implement a new rule, effective November 1998, requiring airport operators and air carriers to audit background investigations for compliance with requirements. As a result of FAA's insufficient oversight actions, noncompliance with background investigation requirements continues, and the little assurance background investigations provide, with regard to granting access to secure areas only to trustworthy individuals, is further weakened.

Improvements Needed in Airport Operator Procedures to Account for Airport ID

At the 6 airports reviewed, 9 percent (234 of 2,586 reviewed) of the IDs issued remained active even though the employee no longer needed the access. The discrepancies were due to air carriers and airport users not notifying the airport immediately when an employee no longer needed access. The discrepancies were also due to airport operators not establishing or implementing adequate controls, such as reviews to verify the accuracy of data provided the airport and assessment of penalties for failing to comply with reporting requirements. As a result, secure areas at those airports were vulnerable to unauthorized access.

FAA plans to issue revised regulations requiring airport operators and air carriers to audit active airport IDs at least once a year. We support this initiative. However, FAA must also issue standard audit procedures to ensure the audits are effective. Procedures should include: maximum time for employers to respond to airport data requests, cancellation of employee access when employers fail to respond to data requests, steps to verify the accuracy of data provided to the airport, and assessment of penalties for noncompliance. FAA must also adequately oversee compliance with requirements to account for airport ID.

RECOMMENDATIONS

We made recommendations to FAA to improve controls over issuing and accounting for airport ID, including:

- Strengthen background investigation requirements to include initial and randomly recurring FBI criminal checks for all employees.

- Expand the list of crimes that disqualify an individual from unescorted access to secure airport areas.

- Incorporate in background investigation requirements the use of credit checks and drug tests to help assess whether individuals can be trusted with the public's safety and be permitted to work in secure airport areas.

- Ensure airport operators and air carriers implement regulations requiring preliminary reviews and audits of background investigations.

- Improve the adequacy and timeliness of guidance provided to FAA regions and field offices on requirements for issuing airport ID, and continue to work with airport operators and air carriers to ensure compliance with requirements.

- Conduct complete assessments of compliance with requirements for issuing airport ID. Assessments should include sufficient testing and use standard methodologies to ensure that data collected in the field can be used to identify and correct systemic problems.

- Issue the proposed revisions to Title 14, Code of Federal Regulations, Section 107 and Section 108, requiring airport operators and air carriers to audit active airport IDs. Also, issue standard audit procedures to ensure the audits are effective.

- Continue to work with airport operators and air carriers to improve compliance with requirements for accounting for airport ID.

- Conduct complete assessments of compliance with requirements for accounting for airport ID. Assessments should include sufficient testing, and use standard methodologies to ensure that data collected in the field can be used to identify and correct systemic problems.

MANAGEMENT RESPONSE AND OIG COMMENTS

FAA concurred with eight recommendations and partially concurred with one recommendation. FAA stated that it has long been concerned about the effectiveness and efficiency of current background investigation requirements and wants them to be improved. FAA plans to propose 100 percent fingerprinting and expand the list of disqualifying crimes with or without legislation.

Also, effective May 31, 2000, FAA amended airport and air carrier security programs to require audits of background investigations and is developing additional written guidance on background investigation requirements. In February 2000, FAA initiated a broad-scoped audit of requirements for issuing airport ID and is working to improve compliance with requirements. As of August 10, 2000, 9,612 employee files were reviewed at 55 major airports.

FAA plans to issue final rules requiring airport operators and air carriers to periodically audit airport IDs, and issue standards and procedures to ensure the audits are effective. FAA began a national employee ID accountability audit in February 2000 and plans to issue field guidance for conducting FY 2001 audits. Further, FAA stated that when new regulations for ID accountability are effective

it will conduct complete assessments of compliance. In the meantime, audits will focus on increasing compliance in this area.

FAA partially concurred with the draft report recommendation to incorporate the use of foreign criminal checks, credit checks, and drug tests to help assess whether individuals can be trusted with the public's safety and be permitted to work in secure airport areas. FAA stated that there are significant problems with conducting and using foreign criminal checks. Based on FAA's comments, we revised our final report and removed that portion of the recommendation related to using foreign criminal checks in background investigations. FAA stated that it would work with Congress, industry, and the law enforcement community to determine if credit checks and drug tests can be fully or partially implemented. However, FAA needs to provide a target date for implementing any requirements for using credit checks and drug tests in employee background investigations.

FAA's actions taken or planned are responsive to all the recommendations and if properly implemented should improve controls over airport ID. However, FAA did not provide estimated completion dates for corrective actions for all the recommendations. We requested FAA provide the estimated completion dates within 15 days.

TABLE OF CONTENTS

I. INTRODUCTION

Background

U.S. airport operators are required to implement Federal Aviation Administration (FAA)-approved security programs. The security programs must include a system, method or procedure for controlling access to the secured area[1] that: (1) ensures only authorized individuals gain access to secured areas; (2) immediately denies access to individuals whose authority changes, such as former airline employees; (3) differentiates between individuals with unlimited access to the secured area and individuals with only partial access; and (4) has the capability of limiting an individual's access by time and date. Over 450 airports are subject to the requirement and have FAA-approved security programs.

To ensure that only authorized individuals gain access to secure areas[2], airport operators and air carriers are required to conduct employment history investigations (background investigations) before issuing airport identification media (airport ID). To ensure that access to secured airport areas is denied immediately to individuals whose authority changes, airport security programs must include a process requiring immediate notification when employees[3] no longer require access.

> Throughout the report we use the term air carriers to mean domestic air carriers.
>
> OIG defines **"airport ID"** as all media issued to individuals to permit access to secure areas.

[1] The **secured area** is the portion of an airport where passengers board and deboard aircraft, and the area surrounding the aircraft. In terms of access control, it must be the most secure area within the Air Operations Area.

[2] OIG defines **"secure area"** (versus secured area) as the area of an airport where each person is subject to a background investigation and required to display airport-approved identification. Each airport defines this area, which may be the entire Air Operations Area or may be limited to a smaller, more restrictive area.

[3] In this report, we use the term employees to mean all individuals authorized unescorted access to secure airport areas, whether these individuals are employed by airports, air carriers, or other entities conducting business at airports.

Objective, Scope and Methodology

The objective of the audit was to determine whether FAA requirements were adequate to ensure that only individuals who could be trusted as guardians of public safety were granted access to secure airport areas. We also assessed FAA's oversight of airport operator and air carrier procedures for issuing and accounting for airport ID. Further, we reviewed airport operators', air carriers', and airport users' compliance with airport ID requirements.

Airport users include foreign air carriers, non-air-carrier airport tenants, and companies that do not have offices at the airport, but require access to the airport's secure area. These include security firms, and food and cleaning service companies.

We reviewed FAA's assessments of airport operator and air carrier compliance with requirements for issuing and accounting for airport ID for fiscal years (FY) 1997, 1998, and 1999. We tested airport operator and air carrier compliance with requirements for issuing and acccounting for airport ID at six judgmentally selected airports. At each airport we randomly selected 10 companies (including the airport operator, air carriers, and airport users) with employees working in secure airport areas. For each company we randomly selected a maximum of 20 background investigation files[4] of employees issued airport ID who were subject to background investigation requirements effective January 31, 1996. Each file (482 total for the 6 airports) was reviewed for compliance with background investigation requirements. Also at each company selected, we compared the airport's list of employees holding active airport ID with the company's list to determine whether access to secure airport areas was immediately denied when employees no longer required access.

We performed the audit in accordance with Government Auditing Standards prescribed by the Comptroller General of the United States. The audit included such tests of procedures and records as were considered necessary in the circumstances.

The audit was performed during the period July through December 1999, and covered the period January 31, 1996, through December 6, 1999. We presented the results of our audit at hearings on March 16, 2000, before the Subcommittee on Aviation, Committee on Transportation and Infrastructure,

[4] If a company in our sample had fewer than 20 employees that fit our criteria, all files were reviewed.

U.S. House of Representatives, and on April 6, 2000, to the Subcommittee on Aviation, Committee on Commerce, Science, and Transportation, U.S. Senate.[5] The audit was performed at the FAA offices and airports listed in Exhibit B.

II. PROGRAM DESCRIPTION

In the 1990's, the Office of Inspector General (OIG) reported on various aspects of aviation security, including airport access control. However, the OIG has not reported on requirements for issuing and accounting for airport ID. Also in the 1990's, Presidential commissions have reviewed and reported on critical aviation issues, including security. In response to the OIG and commission recommendations to improve aviation security, FAA issued new rules to address security weaknesses, including requirements issued in 1995 and 1998 to conduct employee background investigations. Also, as part of its Strategic Plan, FAA has a goal "to eliminate security incidents in the aviation system." However, FAA had not established specific goals related to issuing and accounting for airport ID.

President's Commission on Aviation Security and Terrorism

In response to the December 1988 destruction of Pan Am Flight 103, President Bush established the President's Commission on Aviation Security and Terrorism (Commission) to assess the overall effectiveness of the U.S. civil aviation security system. The Commission's May 1990 report presented recommendations intended to improve the system. One recommendation was for Congress to enact legislation requiring a Federal Bureau of Investigations (FBI) criminal record check (criminal check) for airport employees. Another recommendation was for legislation to identify disqualifying crimes representing a potential security risk.

The Commission's recommendations formed the basis of the Aviation Security Improvement Act of 1990, Public Law 101-604. Section 105(a) of this Act directed the Federal Aviation Administrator (Administrator) to promulgate regulations subjecting individuals with unescorted airport access to employment investigations, including a criminal check, as the Administrator determines necessary. The law included a list of 24 disqualifying crimes. FAA was given the authority to specify other

[5] Aviation Security: Federal Aviation Administration (Report Number AV-2000-070, March 16, 2000, and Report Number AV-2000-076, April 6, 2000).

factors that would help determine whether an individual was ineligible for access to secure areas.

In February 1992, FAA issued a Notice of Proposed Rulemaking (NPRM) to implement Section 105(a). FAA proposed requiring a criminal check for all individuals with unescorted access privileges. FAA also listed the 24 crimes that would disqualify individuals from having airport ID and requested comments on expanding the list.

During the comment period to the NPRM, the overwhelming majority of commenters opposed the proposal based on its cost, the impracticality of escorting personnel while waiting for the results of a criminal check, and the lack of evidence showing a connection between past criminal behavior and future terrorist activity. In the past, processing fingerprints and performing the criminal check took up to 90 days. Some commenters, including the Director of the FBI and the Assistant Attorney General for the Department of Justice's Criminal Division, recommended expanding the list of disqualifying crimes.

Taking into consideration the legislative mandate and the comments received during the rulemaking process, FAA issued a Final Rule, "Unescorted Access Privilege," on October 3, 1995. The rule requires criminal checks only when specific conditions are identified. Individuals convicted within the past 10 years of any of 25[6] enumerated crimes (see Exhibit A for FAA's list of disqualifying crimes) are denied airport ID.

Conditions that trigger an FBI criminal check are (1) an unexplained gap of employment for 12 months or more, (2) inability to substantiate statements made, (3) significant inconsistencies between information provided by the applicant and information obtained during the background investigation, and (4) information becomes available during the background investigation indicating a possible conviction for a disqualifying crime.

The Final Rule also permitted airport operators to accept self-certification from airport users that background investigations were performed: it did not require airport operators to establish controls, such as reviews or audits, to ensure compliance with requirements. Therefore, some airport users with little or no expertise or training were given the responsibility to conduct

[6] Only one crime, felony arson, was added to the list after the NPRM comment period.

background investigations. Air carriers were required to self-certify to the airport operator that background investigations were performed.

White House Commission on Aviation Safety and Security

The July 1996 crash of TWA Flight 800 was the catalyst for important advances in aviation security. Although the FBI and the National Transportation Safety Board ruled out terrorist activity as a potential cause of the crash, the crash prompted the August 1996 creation of the White House Commission on Aviation Safety and Security (Gore Commission). In its February 12, 1997 final report, the Gore Commission recommended "criminal background checks and FBI fingerprint checks for all [airport] screeners, and all airport and airline employees with access to secure areas."

The Gore Commission's recommendations were partially addressed in the Federal Aviation Reauthorization Act of 1996, Public Law 104-264. Section 304 of this Act directed the Administrator to require employment investigations, including a criminal check, for screeners, screener supervisors, and other individuals who exercise security functions associated with baggage or cargo, as determined to be necessary by the Administrator. However, the criminal record check was only required when one of the four special conditions was identified.

Taking into consideration the legislative mandate, FAA issued a Final Rule, "Employment History, Verification and Criminal History Records Check," effective November 24, 1998, requiring background investigations for screeners and their supervisors. Additional revisions included requirements for airport operators and air carriers to audit background investigations and airport operators to conduct preliminary reviews of background investigations performed by airport users.

Government Performance and Results Act

In accordance with the Government Performance and Results Act of 1993, FAA established safety and security goals, objectives, and outcome-based performance measures. However, FAA has not established safety and security goals, objectives, and outcome-based performance measures related to issuing and accounting for airport ID. According to FAA, establishing an appropriate index for these measures is a priority.

III. FINDINGS AND RECOMMENDATIONS

Controlling access to secure airport areas has been, and continues to be, an area of great concern due to increased threat to U.S. airport facilities. Two important access control requirements are to limit access to secure airport areas to individuals who can be trusted with the public's safety and to immediately deny access when an individual's authority changes. FAA has not taken adequate steps to ensure these requirements are met.

We found that improvements are needed in FAA requirements for issuing airport ID. Also, airport operators and air carriers had not complied with requirements for issuing airport ID, and FAA had not taken effective and timely actions to ensure compliance. Further, we found airport operators had not developed and implemented adequate procedures to account for airport ID and immediately deny access to secure airport areas when required.

Finding A. Improvements Needed in FAA Requirements for Issuing Airport ID

FAA requires airport operators and air carriers to conduct background investigations before issuing airport ID. The background investigations include: obtaining a 10-year employment history from those applying for access; verifying the most recent 5 years of that history; and, when one of four specific conditions are identified, performing an FBI criminal check. Individuals convicted within the past 10 years of any of 25 enumerated crimes are denied airport ID.

FAA's Regulations Were Ineffective

Background investigations based on FAA's regulations prove, in most cases, only the identity of the person applying for airport ID and, in limited instances when a criminal check is required, whether the FBI has a record of conviction for a disqualifying crime within the past 10 years. They do not provide adequate assurance that the individual can be trusted with the public's safety, which is the intended purpose of conducting background investigations. We found the following deficiencies in FAA's background investigation regulations.

- ***FBI criminal checks were only required for individuals applying for airport ID when one of four conditions triggers the checks.*** For example, one of the triggers, a 12-month unexplained gap in employment,

was intended to identify individuals who were incarcerated for committing a serious crime. However, according to the U.S. Department of Justice statistics, published in 1999, 61 percent of all state and Federal felony convictions resulted in probation or an average jail sentence of 6 months. Even for violent felony convictions, 43 percent resulted in probation or an average jail sentence of just 7 months.

The ineffectiveness of using an unexplained 12-month gap to trigger an FBI criminal check was highlighted when one of the Nation's largest airports initiated a fingerprint program in 1996. Of the 2,369 individuals who submitted fingerprints for FBI processing, 490 (21 percent) had criminal records, including 41 who had committed 1 or more disqualifying crimes. If the 4 FAA special conditions had been used as triggers to determine who should be fingerprinted, only 2 of the 41 individuals would have been identified and denied unescorted access. These figures do not include individuals (approximately 2 percent) who came to be fingerprinted but left after reading the list of disqualifying crimes.

- ***The list of 25 crimes that disqualified an individual from being issued airport ID was insufficient and did not include serious crimes, such as assault with a deadly weapon, unarmed robbery, burglary, larceny, and possession of drugs.*** The list of crimes that disqualify an individual from being issued airport ID is incomplete because it does not include all crimes that could predict an individual's lack of concern for airport security and the flying public's safety. FAA stated in the 1995 Final Rule:

  > . . . acts of criminal violence, air piracy, and terrorism . . . are neither simple nor uniform, and are certainly not limited to sophisticated acts of international terrorists with political motives or acts of deranged individuals. Also of concern are individuals deliberately committing, or deliberately or unknowingly assisting in the commission of criminal acts against aviation for financial gain or reprisal. . . . A trust is placed in individuals authorized to have access [to secure airport areas], and it is reasonable to establish measures to reduce the likelihood that they present a security risk to civil aviation.

  Our analysis of 53 employees issued airport ID who were arrested in a recent Department of Justice airport investigation for smuggling contraband on commercial aircraft, showed that individuals convicted of

disqualifying crimes were not the only employees who presented a security risk. Of the 15 (28 percent) arrested employees with FBI criminal records, just 1 had a criminal record for a disqualifying crime (committed after being issued airport ID). Other arrested employees (14) had FBI criminal records for non-disqualifying felonies, such as larceny, battery, possession of a stolen vehicle, possession of drugs, and credit card fraud.

- ***FBI criminal checks were not recurring.*** FAA does not require recurring criminal checks but relies on air carriers, airport users, and employees to report employees convicted of disqualifying crimes to airport operators so that access to secure areas can be immediately denied to those individuals. Our analysis of the 53 employees arrested in the recent Department of Justice investigation found that 9 employees were charged with crimes after being issued airport ID, including 1 individual charged with a disqualifying crime. Criminal checks must be recurring to ensure the continued trustworthiness of employees.

- ***Other background investigation procedures, such as credit checks and drug tests, were not used to assess whether employees should be issued airport ID.*** As shown by the recent Department of Justice investigation, 38 of the 53 employees arrested for smuggling did not have criminal records when they applied for airport ID. Therefore, FAA, in cooperation with industry, should develop other initiatives to strengthen background investigation requirements.

  The Canadian Security Intelligence Service conducts credit checks when an individual has been convicted of certain criminal offenses. The results of the checks are considered when determining whether airport ID should be issued. Based on the results, further investigation of the individual's background may be required to determine whether the credit problems were caused by behavioral problems, such as gambling, alcohol, and drug abuse indicating poor judgment, financial irresponsibility, or deceit.

  Credit checks of potential or current employees may be requested by U.S. employers provided it is for a legitimate employment purpose and the individual consents to the credit check. To ensure fairness in requiring credit checks, FAA needs to establish well-defined procedures for when and how to use credit check results to determine whether an individual can be trusted.

  Drug testing would also be a useful tool in determining whether an individual can be relied on to safeguard the flying public. FAA requires

drug testing for employees in "safety sensitive" positions, such as aircraft maintenance workers, flight crews and screeners, but excludes other employees, such as baggage handlers, aircraft cleaning crews and food service providers. As of September 12, 1998, the U.S. Postal Service, which routinely uses commercial air carriers to transport mail, requires individuals who have access to the mail to obtain a security clearance. The clearance includes a required drug test to be completed within 90 days prior to having access to the mail.

A recent OIG investigation at one major U.S. airport resulted in the arrests of three airport employees who used, or allowed others to use for cash, their airport IDs to enter secure airport areas and smuggle drugs onto aircraft. One of the arrested employees had a criminal record for possession of drugs, and other non-disqualifying crimes, prior to applying for airport ID.

To supplement FAA's regulations, some airport operators, air carriers and airport users developed their own background investigation methods that included local criminal checks. Also, one airport we reviewed included a name check through the National Crime Information Center (NCIC) to determine an individual's criminal background. According to the airport's Deputy Director for Public Safety, FAA's requirements are inadequate and the airport had to develop its own policy to ensure the public's safety. The airport's use of the NCIC system for this purpose is contrary to FAA and the Criminal Justice Information Services Advisory Board[7] policies because name checks do not provide the accuracy and completeness of fingerprints.

Another airport recently took steps to supplement FAA's regulations. The airport operator drafted a county ordinance that authorizes the airport to conduct criminal checks and/or financial background checks, and any other background check deemed necessary, for all airport ID applicants and current employees. The ordinance also expands the list of disqualifying crimes to include: cargo theft; smuggling; possession with intent to sell or distribute, sale or trafficking of narcotics or any other controlled substance; dishonesty, fraud, or misrepresentation; and violent crimes committed with a weapon. The criminal checks cannot be processed through FAA because it is against current regulations, nor can the criminal checks be processed directly through the FBI. Therefore, the airport operator plans to inventory the fingerprints until FAA's regulations are changed.

[7] The Advisory Board makes NCIC policy recommendations to the Director of the FBI.

In our opinion, the steps taken by some airport operators to supplement FAA's background investigation regulations are warranted. However, they can only have limited value because vulnerabilities at any one airport can affect the integrity of the entire aviation system nationwide. Therefore, strengthening background investigation requirements must be done nationwide.

FAA has the authority to require criminal checks for all employees and expand the list of disqualifying crimes. However, in the past a criminal check took up to 90 days and, therefore, was not practical or cost efficient. Today, technology allows this process to be completed in only a few days, making it feasible, and in our opinion an appropriate measure. Another reason that criminal checks were opposed when first proposed by FAA was the lack of evidence showing a connection between past criminal behavior and future terrorist activity. However, recent Department of Justice investigations involving employees taking money for placing contraband on aircraft or allowing others to use their airport ID to place contraband on aircraft, have illustrated a connection between past criminal behavior and potential harm to the flying public.

In October of this year, Congress considered and passed the Airport Security Improvement Act of 2000 (Public Law 106-528) which was signed by the President on November 22, 2000. The legislation requires criminal checks for all employees and expands the list of disqualifying crimes. FAA and the airport industry have stated support for the legislation. We also support the initiatives, and recommend that new rules include initial and randomly recurring criminal checks for all employees and that FAA expand the list of disqualifying crimes.

In addition to requiring recurring criminal checks, FAA, in cooperation with industry, should explore other initiatives to strengthen background investigation requirements. For instance, credit checks and drug tests should be considered for use as investigative tools. Some U.S. and foreign jobs require these types of checks and tests to help determine the trustworthiness of employees. The deterrent value alone that would be associated with these requirements cannot be overstated.

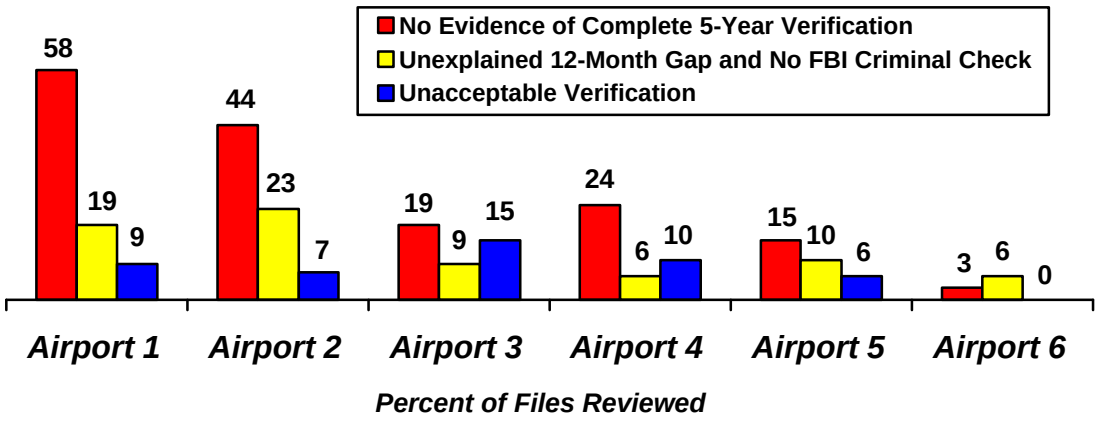
Airport Operators, Air Carriers and Airport Users Did Not Comply With Background Investigation Requirements

Current background investigation requirements must be complied with until FAA issues new background investigation regulations. At the six airports reviewed, we determined that, for 35 percent of employees issued airport ID,

the airport operator, air carrier or airport user had (1) no evidence that a 5-year history verification was conducted (16 percent), (2) incomplete evidence that a 5-year history verification was conducted (16 percent), or (3) no file available for review (3 percent). Also, 15 percent of the files reviewed had an unexplained gap of employment of 12 months or more, but the required FBI criminal check was not performed. Further, 9 percent of the verifications used an unacceptable method, such as verifying an employee's background with a personal reference or family member.

Airport Users and Air Carriers That Self-Certify Background Investigations Were Performed Were the Primary Source of Noncompliance. The most serious deficiencies were at airports that permitted airport users to self-certify that background investigations were performed but which had not established necessary controls to ensure compliance, such as making preliminary reviews of the 10-year employment history and requiring evidence that a 5-year verification was completed. Air carriers[8] also had significant deficiencies. The following chart summarizes our results at the six airports reviewed.

Rates of Noncompliance



- Airports 1 and 2 had high rates of noncompliance. Both airport operators permitted airport users to self-certify background investigations were performed, but had not established controls to ensure compliance. The

[8] Air carriers are required to self-certify to airport operators that employee background investigations have been completed.

background investigations we randomly selected for review were performed by air carriers or airport users.

- Airport 3 permitted some airport users to self-certify that background investigations were performed but the airport did not have adequate controls to ensure the investigations were completed. However, the airport operator performed background investigations for airport users who directly contracted work with the airport (as opposed to those who contracted with air carriers). All background investigations we randomly selected for review were either performed by the airport operator or airport users.

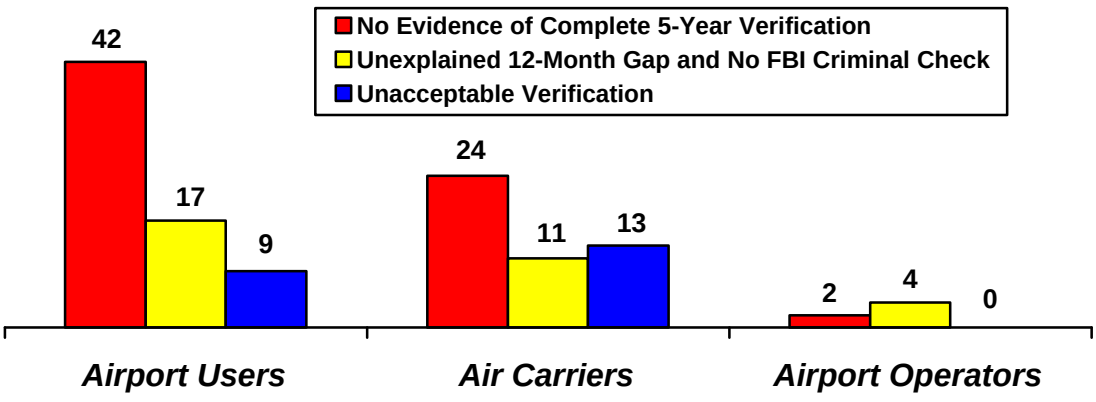
- Airport 4 performed a preliminary review to ensure that a 10-year history was provided. When we reviewed the employer's files, there was not always additional information as evidence that a verification was performed. As a result, Airport 4's rates of compliance were not much better than airports without adequate controls. The background investigations we randomly selected for review were performed by air carriers or airport users.

- Airport 5 performed a cursory review to ensure there was evidence a verification was performed. Therefore, its compliance rates were better than Airport 4. However, deficiencies were still found due to hastily performed reviews. The background investigations we randomly selected for review were performed by air carriers or airport users.

- Airport 6 performed all background investigations for airport user employees and had the lowest rates of noncompliance. No air carrier employees were included in our random sample; therefore, all background investigations we reviewed were performed by the airport operator.

To confirm that the main sources of noncompliance were airport users and

Rates of Noncompliance



air carriers who self-certify that background investigations were performed, we segregated the results by whether the background investigations were performed by airport users, air carriers or airport operators. As shown in the chart below, we found substantially lower rates of noncompliance in each category when airport operators performed the background investigations.

OIG investigations have also found problems with airport users that self-certify background investigations were performed. Two recent investigations, conducted in cooperation with FAA, resulted in fining two companies doing business at major U.S. airports for falsely certifying that background investigations were performed when, in fact, they were not. One of the companies supplied security staff for an airport, and was ordered by a U.S. District Judge to pay more than $1.5 million for allowing untrained employees, some with criminal backgrounds, including drug dealing, kidnapping, aggravated assault and theft, to operate security checkpoints.

FAA Had Not Taken Effective and Timely Actions to Ensure Compliance

We found FAA's national assessments of compliance with background investigation requirements mainly focused on airport users at 20 major U.S. airports and corrective actions were not always effective at the airports we reviewed. Air carrier compliance with background investigation requirements was not formally reviewed until FY 1999. Also, FAA's annual airport assessments of compliance with background investigation requirements need improvement. Further, FAA was slow to implement new requirements and consistently failed to issue timely and adequate guidance to implement existing background investigation requirements.

National Reviews Were Not Always Effective. In 1996, 1997, and 1998, FAA conducted national reviews of airport users' compliance with background investigation requirements.

- The 1996 review included all 19 Category X airports and 22 Category I airports.[9] The objective of the review was to obtain a quick sense of the industry's level of compliance with requirements and was limited to approximately two airport users at each airport.

[9] Category X airports represent the Nation's largest and busiest airports as measured by the volume of passenger traffic and are potentially attractive targets for criminal and terrorist activity. Category I airports are somewhat smaller airports with an annual volume of at least 2 million passengers. At the time of FAA's national reviews and our audit fieldwork, there were 19 Category X airports and 60 Category I airports.

- The 1997 review included 13 Category X airports and 6 Category I airports. A total of 89 companies (ranging from 1 to 18 airport users per airport) and 1,154 files (ranging from 11 to 160 files per airport user) were reviewed at the 19 airports.

- The 1998 review included 17 Category X airports and 1 Category I airport. Approximately 20 airport users and 6 files per airport user were reviewed at each airport.

For each of the three reviews, FAA reported that airport users failed to conduct background investigations, conducted incomplete background investigations, and authorized access to secure areas prior to conducting background investigations.

Despite these findings, we found problems continued with respect to airport users' compliance with background investigation requirements. For example, two of the five airports we reviewed that permitted airport users to self-certify were included in FAA's reviews for at least two of FAA's three reviews. We found significant problems at both airports due to inadequate controls over airport users. The deficiencies persisted because FAA did not ensure corrective actions were taken to address the systemic problems.

To illustrate, one airport was included in all three national reviews. After the 1997 review, FAA recommended the airport conduct audits of airport user compliance with background investigation requirements but the airport refused, stating it was not necessary. FAA made the same recommendation after the 1998 review and the airport agreed to conduct its own audit. However, the audit had not been performed at the time we performed our review in October 1999.

Air carrier compliance with background investigation requirements must be reviewed on a national or regional basis because employee records are generally not maintained at each airport location. However, FAA had not conducted any formal reviews of compliance until FY 1999. As of February 2000, FAA had completed reviews of 49 air carriers and found discrepancies in conducting background investigations at 67 percent of those companies. FAA initiated enforcement actions against nine of the air carriers.

Annual Assessments Need Improvement. FAA field offices are required to perform annual airport assessments for all Category X and I airports. According to FAA:

> A Comprehensive (annual) Assessment is a complete review of a regulated party's compliance with all relevant Federal regulations [and] approved security program requirements. . . .

Assessments include 11 areas that FAA agents must review by conducting surveillance, interviewing airport personnel, reviewing documents, and performing tests. Of the 11 review areas, 2 pertain to airport ID.

We analyzed annual assessments, with respect to assessing compliance with background investigation requirements, for FYs 1997, 1998 and 1999 for the six airports we reviewed. We found the assessments of compliance with background investigation requirements were not always made or were limited in scope.

- Reviews of background investigations were not always made. For example, two of three annual assessments for one airport did not include any tests of background investigation files to determine compliance with requirements. Also, the airport was not included in any of FAA's national assessments of compliance with background investigation requirements during the 3-year period.

- Reviews of background investigations were limited in scope. For example, at an airport that had more than 3,000 active airport IDs, FAA agents reviewed a total of just 18 background records for completeness and accuracy in 3 annual assessments. Also, the airport was included in just one FAA national assessment during the 3-year period that, according to FAA, was a cursory review. At another airport, agents reviewed the airport operator's audit of background investigations for 2 of the 3 years we reviewed but made no independent review to test for compliance.

FAA needs to conduct complete assessments of compliance with background investigation requirements that include sufficient testing, and use standard methodologies to ensure that data collected in the field can be used to identify and correct systemic problems. After we completed our audit fieldwork, FAA initiated a broad-scoped, national review of airport compliance in FY 2000.

FAA Had Not Issued Timely and Adequate Guidance for Implementing Background Investigation Requirements. FAA was slow to issue guidance

to implement background investigation requirements. In 1985, FAA required airport operators and air carriers to conduct 5-year employment verifications. However, very little guidance was issued to implement the requirement, which was an amendment to airport and air carrier security programs. As a result, employers were left to determine how they should verify an employee's background. At one airport we reviewed, FAA officials assigned to oversee the airport incorrectly contended that verification of employment was not required until FAA issued the background investigation rule in 1995. Therefore, at that airport, some employees issued IDs between 1985 and 1995 may not have had background investigations because the 1995 rule exempted all employees issued airport ID prior to January 31, 1996.

On January 31, 1996, the 1995 rule that incorporated the employment investigation requirement into FAA regulations became effective. However, FAA did not issue guidance to explain the rule until November 13, 1997, almost 2 years later.

Also, on November 24, 1998, a new rule became effective to strengthen controls over background investigations performed by airport users. The rule required a preliminary review of the airport users' investigative files "to ascertain completeness" prior to issuing airport ID. FAA's discussion of the rule, published in the Federal Register on September 16, 1998, stated that airport operators must conduct "a preliminary review of the [employee's background investigation] file to ascertain that it is complete." FAA did not provide additional guidance to ensure FAA region and field personnel, as well as airport operators, understood what was required. As a result, FAA personnel in one region we reviewed were not aware the rule was finalized. Also, the Federal Security Manager assigned to an airport in another region we reviewed did not know the requirement was effective as of November 24, 1998, and the airport's Director of Public Safety had not even heard of the new rule.

As a result of the lack of guidance, three of five airports we reviewed that accepted self-certification from airport users were not making the required preliminary reviews. In addition, the two airports that implemented the requirement performed preliminary reviews differently, and neither ensured there was always sufficient evidence that a 5-year verification was conducted.

FAA Was Slow to Implement New Requirements. In addition to not issuing needed guidance to implement new regulations, FAA was slow to complete steps to implement another regulation that was effective November 1998. The new rule required airport operators and air carriers to audit employee

background investigations for compliance with requirements. According to the new rule, the requirement to audit background investigations must be added to the airport and air carrier standard security programs. However, FAA's December 1998 proposed change to the security programs met with objections from airport and air carrier industry representatives. For example, industry commented that the proposal was unclear and did not define the population to be audited or who was responsible for auditing entities contracted by air carriers. Finally, in May 2000, FAA amended the security programs to require the background investigation audits.

We support the need for airports and air carriers to perform audits of background investigations until FAA requires FBI criminal checks for all employees. While this control should have been included in the original background investigation rule in 1995, based on our experience auditing background investigation files, we also understand the concerns expressed by industry. Auditing airport user employee files that are maintained hundreds or thousands of miles from the airport operator is difficult at best. Requiring the files to be sent to a local site for review compromises objectivity. Also, reverifying the work performed for the investigation is costly in time and dollars. Further, the results of such work must be tempered with the fact that time has passed, previous employers may be out of business, or contact information used to confirm an individual's background may no longer be valid.

We attempted to reverify the background investigations of 156 employees included in our review and were able to make a 100 percent reverification of the employee's previous 5-year history for just 73 (47 percent) individuals. For 22 (14 percent) employees, we could not reverify any of their 5-year history. For the remaining 61 (39 percent) employees, we were able to make a partial reverification. The reasons for not being able to fully reverify an employee's background included the following: the employee was not known by a previous employer, a previous employer could not be contacted, employment data were no longer available, and the contact information was incomplete.

In our opinion, the results of our attempts to reverify background investigations will not differ significantly from the results of future industry audits and FAA reviews. Nor would they differ substantially from the results of initial background investigations currently being conducted. Therefore, the futility of the current background investigation process provides additional support for the immediate change of FAA regulations.

Recommendations

We recommend that FAA:

1. Strengthen background investigation requirements to include initial and randomly recurring FBI criminal checks for all employees.

2. Expand the list of crimes that disqualify an individual from unescorted access to secure airport areas.

3. Incorporate in background investigation requirements the use of credit checks and drug tests to help assess whether individuals can be trusted with the public's safety and be permitted to work in secure airport areas.

4. Ensure airport operators and air carriers implement regulations requiring preliminary reviews and audits of background investigations.

5. Improve the adequacy and timeliness of guidance provided to FAA regions and field offices on requirements for issuing airport ID, and continue to work with airport operators and air carriers to ensure compliance with requirements.

6. Conduct complete assessments of compliance with requirements for issuing airport ID. Assessments should include sufficient testing, and use standard methodologies to ensure that data collected in the field can be used to identify and correct systemic problems.

Management Response and OIG Comments

FAA concurred with all recommendations except one. FAA partially concurred with the draft report recommendation to incorporate in background investigation requirements the use of foreign criminal checks, credit checks and drug tests to help assess whether individuals can be trusted with the public's safety and be permitted to work in secure airport areas.

FAA commented that there are significant problems with conducting and using foreign criminal checks. Based on FAA's comments, we revised our final report and removed that portion of the recommendation related to using foreign criminal checks in background investigations. FAA stated that it would work with Congress, industry, and the law enforcement community to determine if credit checks and drug tests can be fully or partially implemented. However, FAA needs to provide a target date for

implementing any requirements for using credit checks and drug tests in employee background investigations.

FAA concurred with the remaining five recommendations. FAA stated that it has long been concerned about the effectiveness and efficiency of current background investigation requirements and wants them to be improved. FAA plans to propose 100 percent fingerprinting and expand the list of disqualifying crimes with or without legislation. Effective May 31, 2000, FAA amended airport and air carrier security programs to require audits of background investigations, and additional written guidance on background investigation requirements is being developed. Also, in February 2000 FAA initiated a broad-scoped audit of requirements for issuing airport ID and is working to improve compliance with requirements. As of August 10, 2000, 9,612 employee files were reviewed at 55 major airports.

FAA's comments and actions taken or planned were responsive to the recommendations to ensure regulations requiring preliminary reviews and audits of background investigations are implemented, and complete assessments of compliance with requirements for issuing airport ID are conducted. If properly executed, the corrective actions should improve controls over airport ID. These two recommendations are considered resolved subject to the follow-up provisions of Department of Transportation Order 8100.1C.

The planned actions for the remaining three recommendations are acceptable, but FAA did not include estimated completion dates. FAA should provide estimated completion dates for these recommendations, in addition to the recommendation to require credit checks and drug tests, within 15 days of this report.

Finding B. Improvements Needed in Airport Operator Procedures to Account for Airport ID

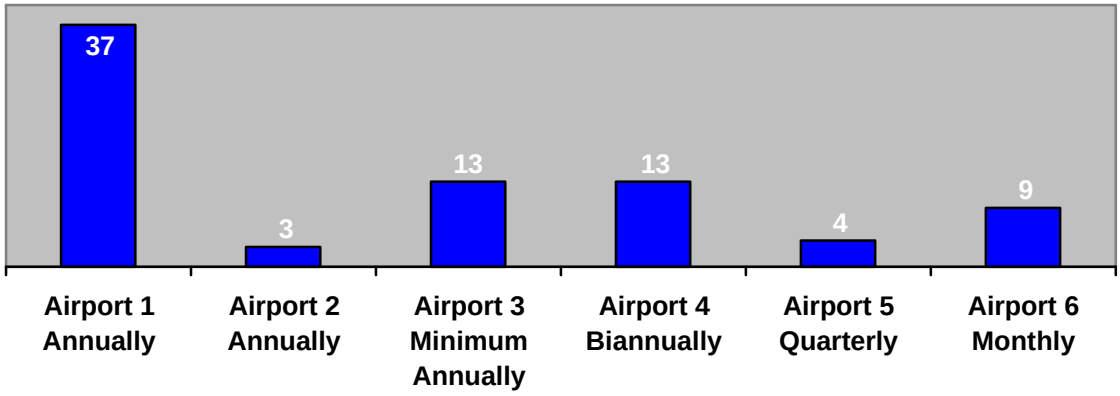
At the 6 airports reviewed, 9 percent (234 of 2,586 reviewed) of the IDs issued to employees for access to secure airport areas remained active even though the employees no longer needed access. The discrepancies were due to air carriers and airport users not notifying the airport immediately when an employee no longer needed access. The discrepancies were also due to airport operators not establishing or implementing adequate controls, such as reviews to verify the accuracy of data provided the airport and assessing penalties for failing to comply with reporting requirements. As a result, secure areas at those airports were vulnerable to unauthorized access.

One of the primary requirements of an airport's access control system is the ability to immediately deny access to individuals whose authority changes, such as previous employees. Effective September 30, 1997, airport operators were required to amend their security programs to require the establishment and implementation of a process to ensure that all air carriers and airport users provide immediate notification when an individual's access authority has been revoked (e.g., the employee resigned or was terminated) or limited (e.g., the job no longer requires access to secure areas).

To assess compliance with FAA requirements, we reviewed airport operator security programs and randomly selected 10 companies, at each of 6 airports, whose employees held active IDs. All six airports had a requirement to audit airport IDs at a specified frequency. The audit processes primarily consisted of mailing lists of active airport IDs to employers for verification on an annual, biannual, quarterly, or monthly basis. However, one airport operator failed to perform audits. None of the other airports performed sufficient tests to verify the accuracy of the data received in response to its audits.

As shown in the chart below, the airport operator that failed to perform audits (Airport 1) had the most discrepancies between the airport's and employers' lists of active airport IDs. However, airports that performed audits also had problems, even when audits were conducted frequently.

Percentage of Discrepancies



The percentage of discrepancies is based on the number of active IDs outstanding for the companies reviewed. The number of active IDs varied based on the companies randomly selected at each airport.

- Airport 1[10] had the highest number of discrepancies (128 of 342). Airport 1 did not perform its required annual audit of airport IDs.

- Airport 2 also had a high number of discrepancies (49 of 1,699). Airport 2 submitted lists of active IDs annually to employers but did not always follow up to ensure verification was received.

> It took more than 3 months for our audit staff to verify Airport 2's list of 881 employees associated with 1 air carrier at the Airport, even though the Airport maintained this process was completed annually.

- Airports 3 and 4 had fewer discrepancies (10 of 76, and 17 of 131, respectively). Airport 3 performed at least an annual audit and reviewed companies known to have problems more frequently. Airport 4 performed a biannual audit.

- Airport 5 also had few discrepancies (2 of 57) and performed quarterly audits. In addition, when IDs were not used to access the airport's automated security system for a period of 30 days, the system automatically voided authorization.

[10] Airport numbers were assigned based on the frequency of audits performed and may differ from previously assigned numbers.

- Airport 6 performed audits monthly and, with the exception of 1 employer, few discrepancies were found (24 of 281).

Airport operators must reissue new airport IDs when 5 percent of the total number of IDs are unaccounted for (i.e., lost, stolen, or not recovered upon termination). This percentage is based on the number of unaccountable IDs reported to the airport by employers and employees. Once reported as unaccounted for, an ID is no longer active and cannot be used to access the airport's automated security system but could be used improperly.

To illustrate, one of the primary components of an airport access control program is for employees to challenge individuals who do not display ID in secure areas of the airport. During our 1998/1999 Audit of Airport Access Control, we were able to penetrate secure areas without wearing airport ID by following employees through access control points. An intruder wearing a lost, stolen, or non-returned ID could easily penetrate a secure area by following an employee through an access control point. Once through the control point, the intruder would have free access on the Air Operations Area, including access to aircraft. For the six airports reviewed, the percentage of unaccountable IDs reported for FY 1999 ranged from 0.4 to 2.8 percent.

The discrepancies we found in our review were in addition to the IDs reported by each airport as unaccounted for and represented IDs that were still active. Therefore, these IDs could have been used to gain unauthorized access through the airport's security system. Any percentage should be viewed with concern, especially when added to the number of unaccounted for airport IDs previously known to the airport, because vulnerabilities at any one airport can affect the entire aviation system.

The discrepancies identified were due to air carriers and airport users not notifying the airport immediately when an employee's authorization changed, as required. Although in some instances the employers maintained the active IDs, others were kept by former employees. For example, a regional air carrier could not account for 22 (18 percent) of 119 active airport IDs. Five of the IDs belonged to employees terminated prior to 1998. Additionally, one airport user failed to report the termination of 14 employees - including 1 employee whose termination was not reported for 1 ½years. The employer could not account for 6 of the 14 IDs. Further, the airport operator found the same problem in 1997 when this airport user had failed to report the termination of 12 employees.

The discrepancies identified were also due to airport operators conducting audits that rely on airport users and air carriers to report discrepancies without the airport operator taking steps to verify the accuracy of data provided the airport. FAA agents generally accepted the airport's audit results without performing steps to verify the results. Further, just one of the six airports we reviewed had established penalties for failing to comply with the requirement to immediately notify the airport operator when an employee's authority changed. However, this airport had not enforced the penalty requirement.

FAA plans to issue a revision to Title 14, Code of Federal Regulations, Section 107 and Section 108 (14 CFR 107 and 14 CFR 108), proposed on August 1, 1997, requiring airport operators and air carriers to audit the number of active airport IDs at least once a year. We support this initiative. However, FAA must also issue standard audit procedures to ensure the audits are effective. Procedures should include: maximum time for employers to respond to airport data requests, cancellation of employee access when employers fail to respond to data requests, steps to verify the accuracy of data provided to the airport, and assessment of penalties for noncompliance. FAA must also adequately oversee compliance with requirements to account for airport ID.

Recommendations

We recommend FAA:

1. Issue the proposed revisions to 14 CFR 107 and 14 CFR 108, requiring airport operators and air carriers to audit the number of active airport IDs. Also, issue standard audit procedures to ensure the audits are effective.

2. Continue to work with airport operators and air carriers to improve compliance with requirements for accounting for airport ID.

3. Conduct complete assessments of compliance with requirements for accounting for airport ID. Assessments should include sufficient testing, and use standard methodologies to ensure that data collected in the field can be used to identify and correct systemic problems.

Management Response and OIG Comments

FAA concurred with all three recommendations. FAA stated the revised 14 CFR Part 107, "Airport Security," and Part 108, "Aircraft Operator Security," will soon be issued. FAA was notified that the Office of the Secretary of Transportation concurred with the new rules on August 8, 2000. FAA plans to issue standard audit procedures to industry as a policy memorandum, subsequent to issuing the new rules.

FAA began a national employee ID accountability audit in February 2000 and plans to issue field guidance for conducting FY 2001 audits. FAA also plans to conduct complete assessments of compliance with the new audit requirements and standard audit procedures after the new rules are published.

FAA's comments and actions taken or planned are responsive to recommendations to continue to work with airport operators and air carriers to improve compliance with requirements for accounting for airport ID, and conduct complete assessments of compliance with requirements for accounting for airport ID. If the corrective actions are properly executed, they should improve controls over airport ID. These two recommendations are considered resolved subject to the follow-up provisions of Department of Transportation Order 8100.1C.

FAA's plan to issue revised regulations and standard audit procedures is also responsive to our recommendation. However, FAA needs to provide estimated completion dates for these actions. FAA should provide the estimated completion dates within 15 days of this report.

Exhibit A

FAA'S LIST OF DISQUALIFYING CRIMES

1. Forgery of certificates, false marking of aircraft, and other aircraft registration violations, 49 United States Code (U.S.C.) 46306
2. Interference with air navigation, 49 U.S.C. 46308
3. Improper transportation of a hazardous material, 49 U.S.C. 46312
4. Aircraft piracy, 49 U.S.C. 46502
5. Interference with flightcrew members or flight attendants, 49 U.S.C. 46504
6. Commission of certain crimes aboard an aircraft in flight, 49 U.S.C. 46506
7. Carrying a weapon or explosive aboard an aircraft, 49 U.S.C. 46505
8. Conveying false information and threats, 49 U.S.C. 46507
9. Aircraft piracy outside the special aircraft jurisdiction of the United States, 49 U.S.C. 46502(b)
10. Lighting violations involving transporting controlled substances, 49 U.S.C. 46315
11. Unlawful entry into an aircraft or airport area that serves air carriers or foreign air carriers contrary to established security requirements, 49 U.S.C. 46314
12. Destruction of an aircraft or aircraft facility, 18 U.S.C. 32
13. Murder
14. Assault with intent to murder
15. Espionage
16. Sedition
17. Kidnapping or hostage taking
18. Treason
19. Rape or aggravated sexual abuse
20. Unlawful possession, use, sale, distribution, or manufacture of an explosive or weapon
21. Extortion
22. Armed robbery
23. Distribution of, or intent to distribute, a controlled substance
24. Felony arson
25. Conspiracy or attempt to commit any of the aforementioned criminal acts

Exhibit B

LOCATIONS VISITED	
FAA Office of Civil Aviation Security	
Headquarters	Washington, DC

FAA Office of Civil Aviation Security Regional Offices	
[redacted]	[redacted]

FAA Civil Aviation Security Field Offices (CASFOs) and Units (CASFUs)	
[redacted]	[redacted]
[redacted]	[redacted]
[redacted]	[redacted]
[redacted]	[redacted]
[redacted]	[redacted]
[redacted]	[redacted]

Airports	
[redacted]	[redacted]
[redacted]	[redacted]
[redacted]	[redacted]
[redacted]	[redacted]
[redacted]	[redacted]
[redacted]	[redacted]

Exhibit C

MAJOR CONTRIBUTORS TO THIS AUDIT

The following staff members were major contributors to this audit:

Robin K. Hunt	Director
A. Robert Lund	Project Manager
Judy W. Nadel	Auditor-in-Charge
Lisa A. Stone	Auditor
Gerald L. Blumenthal	Auditor
Kim P. Tieu	Auditor
James K. Wahleithner	Evaluator

U.S. Department
of Transportation
Federal Aviation Administration

Memorandum

Subject: **ACTION:** Revised Comments to the Office Of Inspector General Draft Report on Controls Over Airport Identification Media

Date: AUG 25 2000

From: Director, Office Civil Aviation Security Operations ACO-1

Reply to Attn. of:

To: Alexis Stefani, Assistant Inspector General for Auditing

Attached are revised ACS comments concerning the Office of Inspector General's (OIG) draft report on the audit on Controls Over Airport Identification Media. These revisions were discussed and agreed to during a teleconference conducted on August 25, 2000. Participating in the conference were myslef and members of our airport operations division (ACO-200), and Ms. Robin Hunt and Mr. Rob Lund of the OIG's San Francisco office.

If you have any questions concerning these revisions, please contact me on (202)267-7262.

Bruce Butterworth

Attachment

ACS REVISED COMMENTS:

Summary: FAA agrees with the OIG that requirements for issuing and controlling IDs that grant access to secured areas of airports need to be strengthened, and that industry compliance needs to be improved. FAA either concurs or partially concurs with all of the OIG's recommendations.

However, in some respects the OIG's report does not take into account FAA's initiative and hard work, nor the legal and practical obstacles FAA faces while attempting to ensure that only persons of integrity have access to airliners and deserve public trust.

The OIG does not fully treat that challenge. Even original and recurrent fingerprint checks for all employees – which FAA supports – cannot ensure integrity. As the example used repeatedly by the OIG demonstrates, only 15 of the 53 employees arrested at one airport had any criminal record at all. For the other 72 percent, only the watchful eye of Federal and local law enforcement and company management can mitigate the risks they present. Criminal history records checks, alone, can not stand as a bulwark against criminal activity directed towards the aviation system. Only a high tempo of activity by law enforcement on airport ramps and the highest vigilance of the employing companies, can preserve the integrity of the system.

These points have been informally presented to the OIG to help the report become the fair, impartial and balanced picture it should be, as required by the Comptroller General's Standards for Government Auditing[11] (see standard 7.58). Still, only some changes have been made in the discussion section and fewer still in the executive summary. Therefore, the same points will be raised again in response to the recommendations and findings of the report.

OIG Recommendation A1: Strengthen background investigation requirements to include initial and randomly recurring FBI criminal checks for all employees.

FAA Response: Concur. FAA has long been concerned about the effectiveness and efficiency of current requirements for verifying the background of persons with unescorted access to the secure area(s) or those conducting screening functions, and wants them to be improved. As evidenced by letters and statements made previously to OIG auditors, FAA will propose 100 percent fingerprinting with or without pending legislation.

OIG Recommendation A2: Expand the list of crimes that disqualify an individual from unescorted access to secure airport areas.

[11] Government Auditing Standards, United States General Accounting Office; 1999 Revision, Amendment No. 2

FAA Response: Concur. Serious crimes that could be disqualifying are not included in the current regulation which includes only those crimes listed by Congress in the Aviation Security Impovement Act of 1990 and arson. On June 1 FAA tasked the Aviation Security Advisory Committee for recommendations on expanding the list of crimes. FAA has also been working with Congress to obtain legislation to expand criminal history record checks and the crimes currently listed in the statute. FAA will propose to amend the regulation with or without additional legislation.

OIG Recommendation A3: Incorporate in background investigation requirements the use of foreign criminal checks, credit checks, and drug tests to help assess whether individuals can be trusted with the public's safety and be permitted to work in secure airport areas.

FAA Response: Partially Concur. FAA believes these ideas have merit and should be considered. However, there are significant problems that the OIG's report does not adequately address. Regarding criminal records, there are *at least* six problems. First, the criminal codes and justice systems of other countries are different from and may even oppose the standard of justice in the United States; in some cases the differences would be impossible to reconcile with U.S. law. Second, some countries do not have fingerprint files and criminal records as we know them. Third, some countries prohibit background investigations by anyone beside that country's police. Fourth, ascertaining how to submit a request for criminal records could be costly and time consuming. Fifth, there is nothing that requires a foreign government to cooperate or respond. Sixth, the results may not serve the purpose of determining "who can be trusted with the public's safety." For example, what credence should be placed in a criminal records check from a state sponsor of terrorism?

Regarding credit checks and drug tests, there are several points that need to be considered. First, credit records are notoriously inaccurate as the circumstances of financial irresponsibility vary widely and a determination would have to be made in each case whether it constitutes a security risk. Making such a determination for the 1.4 million persons who could be subject to the requirement would be substantial. Drug testing would also be a costly endeavor.

Nevertheless, FAA will consider these ideas in light of the practicalities and work with Congress, the industry and the law enforcement community to determine if any of them can be implemented fully or in part.

OIG Recommendation A4: Ensure airport operators and air carriers implement regulations requiring preliminary reviews and audits of background investigations.

FAA Response: Concur. Effective May 31, 2000, FAA amended airport security programs and air carrier standard security programs to require that regulated

parties audit the employment histories and verifications conducted. The first annual self-audit of background investigations begun on February 10, 2000 will be completed by June 30, 2001.

OIG Recommendation A5: Improve the adequacy and timeliness of guidance provided to FAA region and field offices on requirements for issuing airport IDs, and continue to work with airport operators and air carriers to ensure compliance with requirements.

FAA Response: Concur. Since the rule became effective in 1996, FAA has worked vigorously to ensure that its field offices and industry have a common understanding of requirements, and how to resolve the complex questions often raised by employment verifications. For example, a detailed protocol for conducting employment histories and verifications was developed jointly with industry and widely disseminated; the protocol was provided to the OIG. Outreach sessions have been conducted with industry through consortia, and guidance has been provided to the field. Occasional misunderstandings have occurred and FAA will continue to work to ensure a full and common understanding by both field personnel and industry. Although written guidance has been issued to field offices in connection with current national audits, additional written guidance on the various requirements is being developed and will shortly be disseminated to field offices and Federal Security Managers.

OIG Recommendation A6: Conduct complete assessments of compliance with requirements for issuing airport ID. Assessments should include sufficient testing, and use standard methodologies to ensure that data collected in the field can be used to identify and correct systemic problems.

FAA Response: Concur. The FAA has been and will continue to be aggressive in ensuring compliance with the requirements. Since the rule went into effect in 1996, FAA has already conducted three national audits to determine compliance with the criminal history records check rule by airport and tenant employees, and a fourth has been underway since February 2000. Audits to determine compliance by air carriers have been underway since 1999. These audits were in addition to those conducted during routine comprehensive assessments.

The national audits have been directed, primarily, toward the large hub airports that process the greatest numbers of US air travelers. All of these audits have been conducted according to a standardized protocol that is derived from the substantive requirements of the FAA regulation. The testing has consisted of a judgmental sampling of companies whose employees have been authorized unescorted access to airport ramps.

During audits conducted between 1996 through 1999, FAA field reports indicate that 11 airports[12] took remedial action against large numbers or sometimes all employees of entire companies whose employees had unescorted access. The corrective actions involved temporary suspension of unescorted access of large numbers or all company employees until satisfactory background checks and verifications could be properly completed. In addition, at 16 airports[13] FAA field agents conducted 100% audits for the employees of 28 individual airport companies.[14] As a result of these investigations, FAA referred to the OIG three companies for possible criminal investigation, one of which was referred to by the OIG in this report.[15]

Moreover, since February 2000, a fourth national audit has been underway at 55 major airports. As of August 10, 9,612 records were selected at random and reviewed by FAA. Of these records, FAA reverified – by contacting employers – the accuracy of 2,348.

Of the 2,348 available files, FAA found that:

- 83 percent (1,948) were done in full compliance;

- 4 percent (93) were not done at all, with 99 showing discrepancies indicating possible falsification; and

- 13 percent (307) show some degree of inquiry performed by the airport or employer, but with one or more of the following problems: (1) the employee was granted unescorted access prior to verifications being performed, (2) there were unexplained gaps of 12 months or more, (3) there was incomplete biographical information to support the application, (4) there were unacceptable methods of verification.

FAA has also noticed that in many instances the serious problems are common to a single company at a single location. The instances cited above – in which the FAA audited the records of all employees of a single company, or the airport

[12] [redacted]

[13] [redacted]

The conditions at [redacted] were such that the Associate Administrator for CAS issued an Emergency Amendment directing the airport authority to conduct a complete revalidation of all airport id and access control badges in 1999.

[14] 100% audit of records was conducted at [redacted]

[15] [redacted]

had to re-issue badges for all employees of a single company at a single location – substantiate this preliminary conclusion. Despite the FAA's aggressive look at the records of any national company at other airports, once a problem was found at one airport[16], in only two instances was a single company found to have problems at more than one airport. This strongly suggests that serious compliance problems are local rather than national.

FAA's findings long ago strengthened its determination to move as fast as possible to 100 percent fingerprint checks. OIG is correct in concluding that employment verifications are inherently difficult to perform, prone to error, and difficult to audit, for both industry and government.

OIG Recommendation B1: Issue the proposed revision to 14 CFR 107 and 14 CFR 108, requiring airport operators and air carriers to audit the number of active airport IDs. Also, issue standards audit procedures to ensure the audits are effective.

FAA Response: Concur. The soon to be issued final rules for 14 CFR Part 107, Airport Security, and Part 108, Aircraft Operator Security, will establish new regulatory requirements for ID accountability. They will include retrieving expired ID/Access media, reporting lost or stolen media, and auditing the system at least once a year. Revalidating or reissuing ID/Access media will be required if accountability has not been maintained. Standard audit procedures will subsequently be issued to industry as policy memoranda.

OIG Recommendation B2: Continue to work with airport operators and air carriers to improve compliance with requirements for accounting for airport ID.

FAA Response: Concur. Accountability audits will continue through the end of FY 00 and additional guidance will be issued by September to target FY01 audits on this problem.

Beginning in February 2000, FAA security started a national employee ID accountability audit. The audit is conducted according to a standard protocol that requires agents to ensure that airport operators initiate immediate corrective action to address discrepancies uncovered. If warranted, the airport must develop a compliance improvement plan, which includes suspending unescorted access, and revoking, revalidating, or re-issuing IDs.

To date, FAA has audited 19,000 IDs issued to 284 airport *users* of 34 airports.[17] Results thus far show 6% of the *users'* badges are unaccounted for in some respect. However, none of the 34 *airports* show a percentage of unaccounted-for IDs that exceed the FAA maximum percentage of 5% that is allowed before the

16 [redacted]

17 [redacted]

entire ID system has to be revalidated, although in those cases where accountability problems were found, FAA has notified the airport authority for corrective action.

However, airports and companies are not following through on recovery of badges or immediately deleting these badges from the airport's access control databases. Although the 6% is less than the 9% reported by OIG in its audits, FAA recognizes that it points to a gap in compliance in two areas for the affected airports—control of the movement of persons on the ramp, and uncontrolled access through their automated access points.

Until the newly revised rules and implementing guidance are released[18], FAA will use audit efforts to establish a balance between the airports and self-certifying companies in the process of cancellation and recovery of lost, stolen, or unaccounted-for identification and access media. FAA field guidance will be developed and issued by September to guide audits planned for FY 01.

OIG Recommendation B3: Conduct complete assessments of compliance with requirements for accounting for airport ID. Assessments should include sufficient testing, and use standard methodologies to ensure that data collected in the field can be used to identify and correct systemic problems.

FAA Response: Concur. When the new requirements and standard audit procedures are published, FAA will conduct complete assessments of compliance with these new requirements with sufficient testing and standard methodologies. In the meantime, audits will focus on increasing compliance in this area.

FAA currently requires airports to maintain a minimum of 95 percent accountability for active airport issued security identification. When the airport's accountability rate falls below that percentage, then the airport is required to revalidate or re-issue airport identification media. The airports in the US are also required to establish procedures providing for immediate notification by companies and persons when ID and access control media are lost or stolen, when an employee loses unescorted access authority, or upon his or her termination from employment.

When issued, the new regulatory requirements for ID accountability will require the retrieval of expired ID/Access media, the reporting of lost or stolen media, and airport auditing of the system at least once a year. These requirements will ensure proper control over access media.

[redacted]

[18] FAA was notified that OST concurrence was given on 8/10/00

The FAA will then test the strength of airport and air carrier audits. A comprehensive national effort will be initiated as soon as the requirements become disseminated and understood by industry. In the meantime, FAA will continue its current efforts and work with the airport industry to improve local controls over access and ID media.

Additional Comments to OIG Findings

Finding A: Improvements Needed in FAA Requirements for Issuing Airport ID

FAA Comments on Finding: There are several points that need to be included in this section.

First, the record of FAA's efforts to implement criminal history records checks as reported by OIG is incomplete. Industry contested the linkage between commission of the listed crimes and terrorism; although this point is included in the discussion, it is not included in the executive summary. Also, the House Committee on Appropriations, in response to the industry's efforts, restricted funds from being expended to implement the proposed rule. The rule eventually issued has been narrowed under these circumstances. The context of the rule under which FAA now operates needs to be understood.

Second, while the FAA has favored expanded FBI fingerprint checks, advancing a policy of fingerprint checks for all aviation employees depends on reliable evidence that the systems are capable of processing large numbers of fingerprints and criminal history records efficiently. Now, with the increased availability of FBI methods of receiving and transmitting fingerprints via digital networks, FAA is actively supporting the creation of automated fingerprint processing for airports and air carriers. However, there are still major technological and administrative hurdles to cross; and, OIG gives an overly-optimistic picture of progress. High-speed technology and digital automation have been used on a limited basis in an FAA pilot involving four airports and only on those applicants who meet the "trigger" that requires a fingerprint based criminal history check. So far, the pilot is demonstrating that fingerprint results can be completed more efficiently via automation. However, the FAA and industry have not yet tested this application on a wider scale. The national scope of this requirement could grow from several thousand fingerprint submissions annually, since Fiscal Year 96, to more than a million. Current automated applicant processing time has been reported by one airport as taking as long as 10-15 minutes per applicant. This processing time multiplied by 600,000 to 1.4M applicants could represent a significant administrative challenge, and there may be others as well. FAA is determined to work with industry to meet and overcome these challenges, but they must be recognized.

Third, OIG has overlooked a substantive FAA requirement in this area. On July 3, 1996, FAA issued a proposed amendment to the airport security program of every Category X, I, II and III airport that contained procedures for control and accountability of access media and airport-issued ID cards.

Fourth, OIG's summary minimizes the challenge to industry and government to ensure that those who service airliners are worthy of the public's trust. The majority of those caught in recent sting operations had no criminal records whatsoever. The FAA, and the federal government, can only solve part of this problem; law enforcement, both Federal and local, and industry must go beyond Federal requirements and remain vigilant through the execution of corporate and locally based programs.

Fifth, the OIG investigations referred to on pages 14 and 15 were actually initiated because FAA inspections and audits revealed possible criminal activity and FAA referred the case to the OIG. The OIG and FAA worked as teams in these endeavors.